AWARENESS BRIEF

Economic Espionage

Clandestine Methods Used to Disadvantage Canadian Interests

Editor's Note:

This CSIS Liaison / Awareness Brief will be of particular interest to those concerned with the risks to Canadian government and private sector interests posed by the clandestine activities which certain foreign governments may pursue to obtain economic and commercial information.

This brief is published as part of CSIS's national Liaison/Awareness Program. Through this program, the Service seeks to establish ongoing dialogue with organizations, both public and private, concerning the threat posed to Canadian interests by foreign government involvement in economic espionage.

I. Introduction

Economic espionage is damaging Canadian interests at home and abroad. This damage takes the form of lost contracts, jobs and markets, and overall, a diminished competitive advantage. However, the full impact of this activity is difficult to quantify for a number of reasons, including the reticence of companies to reveal the full extent of losses, even when they are known. While not all foreign governments are involved, they all have the potential to commit acts of economic espionage in support of their public and private sector interests. The methods most often employed involve the covert activities of people who have legitimate access to company facilities and information. Vulnerability to acts of economic espionage can be reduced through effective security practices. This paper highlights some of the more common means in which information and technology can be compromised and provides ways in which vulnerabilities can be reduced.

II. Clandestine Access

Employees

Employees may be targeted for their knowledge of, or ability to gain access to, valuable proprietary or sensitive information. For example, employees may be approached for the expertise they personally possess relative to specific scientific work or projects they may be involved in. Similarly, employees with legitimate access to classified government or other sensitive private sector information including reports, passwords (ie: to access computer systems or secure areas) and R&D projects, can be recruited to steal or

copy the information. Motivation on the part of an employee to cooperate with a foreign interest can range from monetary remuneration to revenge, from patriotism to coercion. Employees may also unwittingly cooperate with those clandestinely seeking to acquire information; for example, by providing information to an individual posing as a client or government official.

Foreign governments, including their intelligence services, have the potential either to recruit existing employees and/or facilitate the placement of new employees in particular companies or organizations in order to access specific information. In one example, a Canadian company's technology was compromised when the company, hoping to secure a lucrative contract from a foreign government, accepted a national of that country to work on a sensitive, leading-edge technology project. The foreign government then proceeded to duplicate the technology based on the information obtained through the direct access their national had to this project.

In another case, a foreign national working at a Canadian company was found in possession of restricted R&D and sensitive proprietary data. The individual had entered the premises after hours with an assistant, and together they attempted to steal information stored in electronic databases, which they had spent several weeks correlating. The extent to which company interests were compromised before the individuals were caught has never been determined.

Individuals who intentionally move between companies can gain valuable information and expertise at each job; knowledge which can then be passed or sold to foreign interests.

Contract Employees and Consultants

The use of outsiders, contracted for specific purposes and durations, is a normal part of conducting business today, but represents another avenue through which a company's economic interests may be compromised. As part of a legitimate business agreement, a foreign interest can use contract personnel to gain access to valuable data or information. In one case, a Canadian company discovered two technicians from a foreign state-owned company covertly engaged in trying to obtain proprietary data. The two foreign nationals had been placed in the Canadian facility as part of a contract agreement. Compounding this, an executive from the Canadian company, while visiting the foreign company overseas, believes that his briefcase and documents were compromised while they were left in the "security" of the foreign corporation's office. One target of these activities may have been the Canadian company's contract and subcontracting information. According to the Canadian company, a multimillion dollar contract may have been lost as a result of this activity.

Exchanges

Visiting scientists, technicians, students and delegations are also known avenues by which foreign governments can clandestinely acquire valuable economic information and technology. While this abuse is believed to be limited, it does represent a vulnerable point, particularly as cooperation, joint ventures, between universities, companies and government organizations increase. In one incident, a professor working at a Canadian university on specialized applications for high-energy equipment had his technology stolen. Two foreign exchange students had gained access to the project and the technology they clandestinely acquired was subsequently reproduced in their native country. In a separate incident, a foreign scientist working in the biotechnology sector stole laboratory cultures and confidential company manuals from a Canadian company which is believed to have lost valuable R&D data, as well as potential earnings. It was later determined that the individual involved was implicated in the theft of similar materials from his previous employer.

Members of visiting foreign delegations have also been known to engage in clandestine activities to acquire sensitive information and technology. In one incident, a Canadian company, at the request of a foreign customer, allowed a third country delegation access to its facilities. The delegates took advantage of the visit to covertly acquire company notes and to photocopy technical drawings. This same delegation also attempted, unsuccessfully, to steal a sensitive planning document. In yet another incident, one Canadian company noted instances where visiting delegates from a foreign country tried clandestinely to acquire information from the company. In violation of company security policy which had been

explained to them, one member of the delegation was caught taking pictures inside the facility while another intentionally left the group and was found in a restricted area of the facility with his visitor's pass hidden in a pocket.

Abuse of International Institutions and Organizations

International organizations and institutions play a significant role in furthering cooperation, scientific advancements and mutual economic prosperity. However, some countries abuse exchange opportunities available to them via their membership in international institutes and organizations. Nationals of such countries who are sponsored by an international organization may be accorded privileged and access that, on a bilateral basis, they would not have normally received. The ability of these individuals to abuse their access can be compounded by host organizations, who in the spirit of international cooperation, do not apply the security policies and practices they might normally afford bilateral arrangements. In one such case, a foreign national sponsored by a credible international organization and working at a Canadian research site was suspected of having removed, without authorization, numerous documents containing technical data. While the full extent of material taken remains unknown, the Canadian research organization deemed this a serious loss.

Communications Interception

Governments, business enterprises, research institutes and individuals rely on sophisticated electronic equipment for communications. The interception of these telecommunications, through the use of commercially available equipment, is another method used by foreign interests to obtain proprietary information. Cellular phones, faxes and telephone communications, both domestic and international, have been increasingly targeted for clandestine interception.

Two cases of deliberate telecommunications interception for commercial gain indicate how Canadian companies can be disadvantaged by this type of activity. In the first incident, it was suspected that the host government was intercepting telephone communications between an executive abroad and his Canadian company headquarters. In this respect, Canadian executives on the phone discussing the bottom line price for a contract under negotiation with a foreign government were surprised when this figure became the immediate counter offer put forward by the host organization the following day. In another case, a Canadian business executive suspected that his telephone communications were monitored by a foreign government during contract negotiations when the exact phrasing the executive used in discussions with his Canadian office became part of the negotiation terminology the following day.

Computer systems can also be vulnerable to clandestine access. Information including R&D data, proprietary information, reports, analysis and personnel records contained in computer systems can be the target of foreign interests. In the case of one Canadian company, a protected computer system was compromised by a perpetrator who gained unauthorized access and intentionally tampered with existing computer codes and files. In a separate incident, a foreign government is believed to have tasked its intelligence service to gather specific information. The intelligence service in turn, contracted computer hackers to help meet the objective, in the course of which, t he hackers penetrated databases of two Canadian corporations. These activities resulted in the compromise of numerous computer systems, passwords, personnel and research file of the two companies.

Disposal of Waste Materials

Another avenue of clandestine access to information is the retrieval of an organization's waste material from containers located internally and externally. Discarded business notes, reports, plans, operational manuals and other sensitive data with regular waste materials can offer valuable insight into the inner workings of an organization. One telecommunications organization found its computer programs accessed by individuals who had rummaged through an unlocked dumpster located next to the building, and were then able to retrieve sensitive computer reports and codes which allowed them to traverse all levels of the company's computer systems. In addition, recycling practices have sometimes blurred the importance of proper disposal of sensitive documents. While there is good intent in encouraging environmentally-friendly waste disposal practices, sensitive

documents and reports should be first rendered illegible (ie: shredded) before being recycled. Discarded computer disks that do not have their contents magnetically erased can also provide valuable information.

Business Trips and Other Related Activities Outside Canada

International business activities conducted abroad can result in an increased vulnerability to economic espionage due to the limited amount of control an organization can exercise over the foreign business environment and the more intrusive methodologies a foreign government can use in its own country. The more significant the information may be to a foreign competitor, the more likely the government may be prepared to assist in acquiring the information. In this respect, if the potential gains are significant enough, a variety of methods are available to foreign governments in order to compromise the desired information or technologies. Briefcases and other luggage can be searched and copied covertly on point of entry, exit or at any time during the visit when not under direct control. In addition, foreign hotel rooms, safes and local communication systems are accessible to foreign security and intelligence services.

III. Reducing Vulnerabilities

Canada is a world leader in several fields including aerospace, biotechnology, computer technology and telecommunications. Canadian public and private organizations possess information of both technological and economic significance, the protection of which is essential to their economic well-being, and by extension, the economic interests of Canada. Leading-edge technology, R&D and other sensitive business information are vulnerable to targeting by foreign interests. Canadian organizations are often in the best position to assess the information they must protect and from whom it is to be protected. The following are some security measures which may help reduce the vulnerability of organizations to economic espionage:

- Appropriate classification, control and protection of sensitive documents;
- Protection of computer databases and network links from unauthorized access;
- Identification and controlled destruction of sensitive company waste material;
- Proper storage and disposal of sensitive documents;
- Discussion of sensitive company matters in appropriate locations;
- Full assessments of the value of the information (relative to both the organization and your foreign competitor's interests), the utility of the information being taken abroad, and implementation of security measures commensurate with this assessment, based on the underlying premise that "if you cannot afford to lose it, do not take it with you";
- Realistic controls on employee/visitor access to sensitive facilities, material, etc., based on the "need to know" principle;
- Sensitivity and caution with the choice of medium used for business communications (ie: cellular phones, open fax and phone lines);
- Education and sensitization of all employees to the threat that economic espionage may pose to job security and the organization's economic well-being. Emphasis on sharing responsibility amongst all employees for adherence to effective security policies and practices.

Cooperation between government and business is important to develop and maintain a secure business environment conducive to advancing Canadian economic interests in the global marketplace and reducing the vulnerabilities to economic espionage activities.

April 1998

Comments on this brief are welcome, and should be directed to the National Coordinator, Economic and Information Security, Box 9732, Station "T", Ottawa, K1G 4G4, phone (613) 231-0100, fax (613) 842-1390. If you'd like to talk to CSIS regarding a particular security concern, please contact the local Economic and Information Security Coordinator at one of the CSIS offices listed below:

Newfoundland ..... (709) 772-5449

Nova Scotia ..... (902) 420-5900

New Brunswick ..... (506) 452-3786

Quebec
- Montreal ..... (514) 393-5600
- Quebec City ..... (418) 529-8926

Ontario
- Ottawa ..... (613) 998-1679
- Toronto ..... (416) 865-1480

Manitoba ..... (204) 983-5405

Saskatchewan ..... (306) 780-5512

Alberta
- Edmonton ..... (403) 421-5800
- Calgary ..... (403) 292-5255

British Columbia ..... (604) 528-7400

BULLETIN DE SENSIBILISATION

Espionnage économique

Moyens clandestins employés au détriment des intérêts canadiens

Note de la rédaction :

Le présent bulletin intéressera particulièrement ceux qui se soucient des riques que les activités clandestines de certains pays désireux de se procurer des renseignements de nature économique et commerciale font peser sur les intérêts publics et privés canadiens.

Le présent bulletin est publié dans le cadre du Programme national de liaison et de sensibilisation du SCRS, dont l'objectif est d'établir avec les secteurs public et privé un dialogue permanent sur les menaces aux intérêts du Canada décrites ci-après l'espionnage économique animé par les gouvernements étrangers.

I. Introduction

L'espionnage économique nuit aux intérêts canadiens au pays et à l'étranger. Ce préjudice se traduit par la perte de contrats, de marchés et d'emplois, et en général par une baisse de l'avantage concurrentiel. Les retombées de ce type d'activité sont toutefois difficiles à quantifier pour plusieurs raisons, notamment parce que les entreprises hésitent à révéler l'ampleur de leurs pertes, même lorsqu'elles la connaissent. Bien que les gouvernements étrangers ne soient pas tous nécessairement impliqués, il sont tous en mesure de mener des activités d'espionnage économique pour appuyer leurs secteurs public et privé. Ils ont le plus souvent recours à des gens qui sont en mesure d'accéder en toute légitimité aux installations et aux informations visées. Des mesures de sécurité efficaces peuvent réduire la vulnérabilité à l'espionnage économique. Le présent rapport passe donc en revue certains des moyens les plus couramment utilisés pour obtenir secrètement des informations et de la technologie et propose des mesures à prendre pour être moins vulnérable.

II. Méthodes clandestines d'accès

Employés

Des employés peuvent être pris pour cible soit parce qu'ils sont au courant de précieuses informations exclusives ou de nature délicate, soit parce qu'ils peuvent avoir accès à de telles informations. Ainsi, il arrive que des employés soient pressentis pour profiter de leur expertise dans un domaine scientifique particulier. De même, des employés ayant accès à des informations classifiées du gouvernement ou à des informations délicates du secteur privé tels des rapports, des mots de passe (permettant par

exemple d'accéder à des systèmes informatiques ou à des zones protégées) et des renseignements sur des projets de recherche et de développement, peuvent être recrutés dans le but de voler ou de copier ces informations. Des employés peuvent accepter de coopérer avec des intérêts étrangers pour diverses raisons : argent, vengeance, patriotisme, coercition, etc. Ils peuvent aussi collaborer inconsciemment avec ceux qui tentent d'obtenir secrètement des informations, par exemple en renseignement une personne qui se fait passer pour un client ou un représentant du gouvernement.

Des gouvernements étrangers, y compris leurs services de renseignements, sont en mesure de recruter des employés dans certains sociétés ou organisations ou d'y placer des personnes afin d'obtenir des informations précises. Dans un cas, une entreprise canadienne qui espérait passer un contrat lucratif avec un gouvernement étranger a accepté qu'un ressortissant du pays en question prenne part à un projet de technologie de pointe dans un secteur sensible. C'est ainsi que sa technologie a été compromise, car le gouvernement étranger l'a reproduite en se basant sur les informations acquises par le ressortissant dans le cadre de sa participation au projet.

Dans un autre cas, un ressortissant étranger à l'emploi d'une entreprise canadienne a été surpris en possession d'informations à diffusion restreinte sur la recherche et le développement et de données exclusives de nature délicate. L'individu est entré dans les locaux après les heures de travail en compagnie d'un assistant pour voler des informations qu'il avait passé plusieurs semaines à compiler et qui étaient stockées dans des bases de données électroniques. L'entreprise n'a jamais pu déterminer dans quelle mesure ses intérêts ont été compromis avant que les deux personnes ne soient prises en flagrant délit.

Des personnes qui passent intentionnellement d'une entreprise à une autre acquièrent des informations et des connaissances fort utiles à chacun des postes qu'elles occupent et peuvent ensuite les transmettre ou les vendre à des intérêts étrangers.

Contractuels et consultants

Le recours à des contractuels embauchés à des fins précises et pour des périodes déterminées est chose courante de nos jours dans les entreprises, mais peut mettre en péril les intérêts économiques d'une entreprise. Des intérêts étrangers peuvent, dans le cadre d'accords commerciaux légitimes, faire appel à des contractuels pour avoir accès aux données ou aux informations convoitées. Une entreprise canadienne, par exemple, a découvert que deux techniciens à l'emploi d'une société d'État étrangère tentaient de se procurer clandestinement des données exclusives. Ils travaillent à l'entreprise canadienne dans le cadre d'un contrat. De plus, un cadre supérieur de cette même entreprise soupçonne que sa serviette et ses documents ont été compromis lorsqu'il les a laissés en «sécurité» dans le bureau de la société d'État étrangère où il était de passage. Il se pourrait que des informations sur les contrats et la sous-traitance aient été visées. L'entreprise canadienne croit qu'elle pourrait avoir perdu un contrat de plusieurs millions de dollars à la suite de cet incident.

Étudiants, délégations et scientifiques étrangers

Il est connu que des gouvernements étrangers font aussi appel à des scientifiques, des étudiants et des délégations de passage dans un pays pour acquérir clandestinement des technologies et des informations économiques importantes. Bien que cette tactique semble peu souvent utilisée, elle n'est pas à négliger, surtout à cause des co-entreprises et des projets de collaboration de plus en plus nombreux auxquels participent des universités, des sociétés et des organismes gouvernementaux. Ainsi, un professeur travaillant dans une université canadienne à des applications spécialisées d'équipement à haute énergie s'est fait voler sa technologie. Deux étudiants étrangers participant à un échange ont eu accès à son projet. La technologie qu'ils ont acquise subrepticement a par la suite été reproduite dans leur pays d'origine. Lors d'un autre incident, un scientifique étranger oeuvrant dans le secteur de la biotechnologie a volé des cultures de laboratoire et des manuels confidentiels dans une entreprise canadienne qui aurait ainsi perdu de précieuses données dans les domaines de la recherche et du développement ainsi que des bénéfices éventuels. Il a par la suite été possible de déterminer que ce scientifique avait aussi volé du matériel similaire chez son employeur précédent.

Des membres de délégations étrangères de passage se livrent aussi à des activités clandestines dans le but d'acquérir des informations et des technologies de nature délicate. À la demande d'un client étranger, une entreprise canadienne a autorisé les membres d'une délégation d'un tiers pays à visiter ses installations. Ceux-ci ont profité de l'occasion pour se procurer secrètement des notes et photocopier des dessins techniques. Ils ont aussi tenté en vain de voler un document de planification de nature délicate. Dans le cadre d'un autre incident, une société canadienne a constaté à plusieurs reprises que des membres de délégations étrangères avaient essayé d'acquérir clandestinement des informations. L'un d'eux a été surpris en train de photographier l'intérieur des installations en contravention de la politique en matière de sécurité qui avait été expliquée aux visiteurs tandis qu'un autre, ayant intentionnellement quitté le groupe et caché sa carte de visiteur dans sa poche, a été interpellé dans une zone à accès restreint.

Organisations et institutions internationales

Les organisations et institutions internationales contribuent énormément à l'établissement d'une certaine collaboration aux progrès scientifiques et à une prospérité économique réciproque. Certains pays abusent toutefois des programmes d'échange et de leur appartenance à des instituts ou organismes internationaux. Leurs ressortissants qui sont parrainés par une organisation internationale peuvent se voir accorder des privilèges et un accès qu'ils n'obtiendraient pas normalement dans le cadre d'ententes bilatérales. De plus, les organismes d'accueil qui, dans un esprit de coopération internationale, n'appliquent pas les politiques et les pratiques de sécurité pertinentes, viennent augmenter les risques d'abus. Un ressortissant étranger commandité par une organisation internationale digne de confiance et travaillant dans un centre de recherche canadien est soupçonné d'avoir emporté sans autorisation de nombreux documents contenant des données techniques. L'établissement de recherche n'a pu établir avec précision le nombre de documents qui ont été pris, mais il estime avoir subi de graves pertes.

Interception des communications

Les gouvernements, les entreprises, les instituts de recherche et les particuliers utilisent du matériel électronique sophistiqué pour communiquer. Des intérêts étrangers se servent du matériel disponible dans le commerce pour acquérir des informations exclusives. Les communications intérieures et internationales transmises par téléphone, téléphone cellulaire et télécopieur sont de plus en plus la cible d' interceptions clandestines.

Deux cas dans lesquels des télécommunications ont été délibérément interceptées dans le but de réaliser des bénéfices commerciaux illustrent comment ce type d'activité peut être préjudiciable aux entreprises canadiennes. Dans la première affaire, le gouvernement hôte est soupçonné d'avoir intercepté les conversations téléphoniques entre un cadre supérieur en voyage à l'étranger et le siège social de son entreprise au Canada. Les cadres supérieurs canadiens avaient discuté en détail de certaines négociations avec un gouvernement étranger et notamment d'une offre minimale. Le lendemain, à leur surprise, l'organisation hôte a fait immédiatement une contre-proposition équivalente à l'offre minimale dont il avait été question lors de la communication. Dans un autre cas semblable, lors de négociations contractuelles, un cadre supérieur d'une société canadienne a eu le sentiment qu'un gouvernement étranger avait écouté ses conversations téléphoniques lorsque les propos qu'il avait tenus lors de récentes discussions avec son bureau au Canada ont été intégrés dans les négociations le lendemain.

Les systèmes informatiques peuvent aussi être vulnérables à l'accès clandestin. Les données sur la recherche et le développement, les informations exclusives, les rapports, les analyses et les dossiers du personnel stockés dans ces systèmes peuvent être pris pour cible par des intérêts étrangers. En effet, un système informatique protégé dans une entreprise canadienne a été compromis par une personne qui y a accédé sans autorisation et qui a sciemment trafiqué les codes machines et les fichiers. Dans le cadre d'un autre incident, un gouvernement étranger aurait chargé son service de renseignements de recueillir des informations précises. Pour réaliser son objectif, celui-ci a fait appel à des pirates informatiques qui ont infiltré les bases de données de deux

entreprises canadiennes. Ces activités ont entraîné la compromission de nombreux systèmes informatiques, mots de passe, dossiers du personnel et fichiers de recherche dans les deux sociétés.

Élimination des rebuts

Une autre façon d'avoir accès de manière clandestine à des informations consiste à récupérer les rebuts d'une organisation qui sont jetés dans des contenants placés à l'intérieur ou à l'extérieur des locaux de celle-ci. Les notes d'affaires, les rapports, les plans, les manuels opérationnels et les autres données de nature délicate qui sont mêlés aux rebuts ordinaires peuvent fournir de précieuses informations sur les rouages internes d'une organisation. Ainsi, en fouillant dans une benne à déchets qui n'était pas fermée à clef et se trouvait près de l'immeuble d'une organisation de télécommunications, des individus ont mis la main sur des programmes informatiques et ont pu récupérer des rapports et des codes informatiques de nature délicate qui leur ont permis d'avoir accès à tous les niveaux des systèmes informatiques de la compagnie. Par ailleurs, le recyclage a fait en sorte que l'importance nécessaire n'a pas toujours été accordée à l'élimination des documents de nature délicate. Il est bon d'adopter des pratiques écologiques pour l'élimination des rebuts, mais il faut d'abord rendre illisibles (déchiqueter, par exemple) les documents et les rapports de nature délicate avant de les recycler. Les disquettes d'ordinateur que l'on jette sans en avoir effacer le contenu magnétiquement peuvent également fournir de précieuses informations.

Voyages d'affaires et activités connexes à l'étranger

Les entreprises actives dans d'autres pays deviennent parfois plus vulnérables à l'espionnage économique parce qu'elles ne peuvent exercer qu'un contrôle limité sur un milieu des affairès qui n'est pas le leur et qu'un gouvernement peut utiliser des méthodes plus intrusives sur son territoire. Plus des informations sont importantes aux yeux d'un concurrent étranger, plus le gouvernement risque d'être disposé à l' aider à les obtenir. En conséquence, si les bénéfices éventuels sont suffisamment importants, les gouvernements étrangers peuvent recourir à diverses méthodes pour compromettre les informations ou les technologies convoitées. Les serviettes et les bagages peuvent être fouillés et les documents intéressants reproduits secrètement au point d'entrée ou de sortie ou à n'importe quel moment pendant le voyage, lorsque le visiteur ne les a pas en sa possession. De plus, à l'étranger, les services de renseignements du pays hôte ont accès aux chambres et aux coffres-forts dans les hôtels ainsi qu'aux systèmes de communication locaux.

III. Réduire la vulnérabilité

Le Canada est un chef de file mondial dans plusieurs domaines, dont l'aérospatiale, la biotechnologie, l'informatique et les télécommunications. Les secteurs public et privé possèdent des informations importantes sur les plans technologique et financier qui doivent absolument être protégées pour assurer la santé économique et, partant, les intérêts économiques, du Canada. Les informations sur la technologie de pointe, la recherche et le développement et d'autres informations commerciales de nature délicate peuvent intéresser des intérêts étrangers. Les organismes canadiens sont souvent les mieux placés pour déterminer les informations qui doivent être protégées et contre qui. Des mesures de sécurité peuvent rendre les organisations moins vulnérables à l'espionnage économique :

- Classifier, administrer et protéger adéquatement les documents de nature délicate.
- Protéger les bases de données informatiques et les liaisons entre réseaux contre tout accès non autorisé.
- Déterminer les documents de nature délicate qui doivent être détruits et en superviser l'élimination
- Entreposer et contrôler convenablement les documents de nature délicate.
- Discuter des questions délicates de l'entreprise dans des endroits appropriés.
- Déterminer la valeur des informations (pour l'organisation et pour le concurrent étranger) et l'utilité de celles qui sont apportées à l'étranger puis, en fonction de cette évaluation, mettre en oeuvre des mesures de sécurité qui tiennent compte du fait qu'il ne faut pas prendre avec soi

des informations qu'on ne peut se permettre de perdre.

- Contrôler avec réalisme l'accès des employés et des visiteurs aux installations, aux documents, etc. de nature délicate, en fonction du principe du «besoin de savoir».
- Choisir avec soin et circonspection le mode de communication pour les discussions d'affaires (téléphone cellulaire, téléphone et télécopieur non protégé).
- Sensibiliser tous les employés à la menace que l'espionnage économique peut faire peser sur leur sécurité d'emploi et sur la santé financière de l'entreprise. Mettre l' accent sur le partage des responsabilités entre tous les employés pour que ceux-ci respectent les politiques et les pratiques efficaces adoptés en matière de sécurité.

Le gouvernement et les entreprises doivent collaborer pour rendre le milieu des affaires sûr, favorable à la croissance des intérêts économiques du Canada sur le marché mondial et moins vulnérable à l'espionnage économique, et pour faire en sorte qu'il le reste.

avril 1998

N'hésitez pas à nous faire part de vos commentaires sur ce bulletin. Veuillez les adresser au coordonnateur national des questions de sécurité économique et de l'information, C.P. 9732, Succursale postale «T», Ottawa, K1G 4G4, téléphone (613) 231-0100, télécopieur (613) 842-1390. Si vous souhaitez discuter d'une question particulière, veuillez communiquer avec le coordonnateur des questions de sécurité économique et de l'information de l'un des bureaux régionaux suivants du SCRS :

Terre-Neuve ..... (709) 772-5449

Nouvelle-Écosse ..... (902) 420-5900

Nouveau-Brunswick ..... (506) 452-3786

Québec
- Montréal ..... (514) 393-5600
- Québec ..... (418) 529-8926

Ontario
- Ottawa ..... (613) 998-1679
- Toronto ..... (416) 865-1480

Manitoba ..... (204) 983-5405

Saskatchewan ..... (306) 780-5512

Alberta
- Edmonton ..... (403) 421-5800
- Calgary ..... (403) 292-5255

Colombie-Britannique ..... (604) 528-7400